

With respect to the rejection of Claim 1, as explained in the introduction to the instant application, the element relating to "assignment of predetermined means of access to the device associated with the authentication system," is not predominately access to physical hardware resources, as described by Angelo. In accordance with the present invention, this is also, and primarily, access to different (software) functions, based on the privileges of the user who identified himself/herself to the system.

This is a key differentiation in that Angelo refers only to the usage of the token for the purpose of authentication of the entire system. Angelo implies authentication checks which result in "Full Access" to entire system or no access to the entire system at all. This feature is comparable to a PC's "Power On Password" utilizing a cryptographic token.

The present invention describes more than just the basic access to the entire system (i.e. the computer system described by Angelo). The present invention as described can also be used by a particular Software Application on the system to verify access authorization.

For example, this could be a single software application, which evaluates the security token and is running on top of the used hardware.

Applicants also detail the usage of the token to provide specific configuration information, which defines constraints for the usage of a particular user. This "constraint" e.g. temporary deactivation, limits the usage of a reduced feature set. This is more than just "authentication". It adds "authorization"(!) patterns.

The support for this is disclosure is found at page 15, the last full paragraph:

"A company telephone system consists of 20 telephones hierarchically grouped into three levels, with corresponding scopes of functions. The telephone sets themselves are produced uniformly and are assigned their actual features only by means of the configuration procedure, which enables or disables various logic components in the sets depending on the customer's specific requirements."

Another differentiation between the present invention and Angelo is the scope of usage: Angelo refers to "Computer systems." The Angelo drawings disclose that the computer system refers to a typical Personal Computer System, Workstation or Host system (PCI Bus, video controller, network adapter). The present invention explicitly mentions the usage of the authentication token for various additional devices, such as set-top boxes, etc....

Based on the broad scope of devices, the present invention can be based on a pure hardware (in-vehicle system), OR hardware + firmware programs (phone) OR hardware + software solution (Personal Digital Assistant or Personal Computer).

The present specification states at page 1, lines 12 - 20 which forms the basis for the amendment to Claim 1:

"The term "device" in the context of the inventive concepts presented here is very broad and generalized. It covers a broad variety of equipment from small mobile phones or other small computer-controlled consumer devices with a certain, relatively low, level of computing power, through actual computers, to larger items of equipment such as motor vehicles, all the way up to control terminals for industrial processes, which may require authentication prior to operation."

With respect to the rejection of Claim 2, Angelo is controlling the access to the device. If the authentication according to Angelo is not successful, the user can't access the device.

Claim 2 of the instant application covers basic means of access which comprise at least one of the following means: "Disable operation of the device, enable operation of the device, or enable configuration of the device." In the instant invention, one of the results of the checks could be that the device is disabled (and not just the access is denied, like in Angelo). Also, as already mentioned with regard to claim 1, the present invention also covers the access to functions of the device, not only to physical resource like in Angelo. In claim 2, the configuration mode of the device is one possible software function that we give access to, based on the privileges that the user accessing the device has.

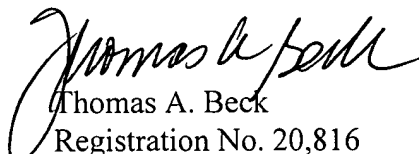
With respect to the rejection of claim 3, relating to “...reading the features...,” there is no clear reference in Angelo, and thus no support for the rejection (clearly not in the lines and drawings cited by the Examiner) that this reading feature is done/disclosed in Angelo without the need for an intermediate software layer. This interpreted out of Fig.1, as there is no software layer mentioned.

As stated above, in the present invention, Applicants intend to deal with manifold devices - even those which do not have typical software, but only firmware provided in a Read Only Memory (e.g. phones).

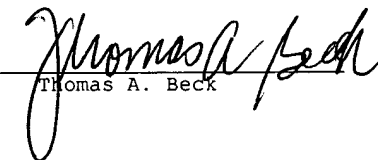
As to the Examiner’s rejection of claim 4, in Column 6, lines 21-31 Angelo mentions the “Token” and describes different cryptographical algorithms that could be used within the token. This is different from what is claimed in claim 4 of the present invention, where Applicants define what could be components of the authentication unit as described in the invention. Although Angelo discloses “Cryptographic algorithms” and “Keys,” these are only two components. Angelo does not disclose firmware programs, device-specific command sequences for execution of specific device-specific functions and individual decision-making logic as being within the scope of his invention. Thus the rejection is improper as Angelo does not disclose each and every element found in Applicants’ claim 4.

In view of the arguments and modifications to the claims, allowance of this case is warranted. If there are additions which could result in the claims being allowed, Applicants' attorney would be pleased to speak with the Examiner by phone concerning such action. Such favorable action is respectfully solicited.

Respectfully Submitted,


Thomas A. Beck
Registration No. 20,816
26 Rock Ledge Lane
New Milford, CT 06776
(860) 354-0892

I hereby certify that this supplemental paper is being deposited on the date indicated below with the U.S. Postal Service as First Class Mail addressed to Commissioner of Patents & Trademarks, Post Office Box 1450, Alexandria, VA 22313-1450

Signature: 
Name: Thomas A. Beck

Date: July 6, 2004

APPENDIX A

1. (Currently amended) A method for setting basic means of access for operation of devices of which the operation is controllable by electronic means, comprising:

said devices comprising mobile phones, small computer-controlled consumer devices with relatively low level of computing power, computers, motor vehicles, control terminals for industrial processes, all of which devices may require authentication prior to operation;

establishment (110) of a link (19) between a personal authentication system (16) supplied with encryption data and a logic system (20) able to control an electronic device control.

checking (120, 140) said encryption data in said authentication system (16) prior to operation of said electronic device control;

assignment of predetermined means of access to said electronic device control associated with said authentication system (16) said predetermined means providing access to physical hardware resources and access to different software functions, based on the privileges of the user who identified himself to the system, said software function evaluates a security token and is running on top of said physical hardware;

enabling (150) of said means for access predetermined for said authentication system (16) dependent on the result of said check.

2. (Currently amended) The method defined in Claim 1, wherein said basic means of access to functions of said device comprise at least one of the following means: disable operation of said devices (12), enable operation of said devices (12), or enable configuration of said devices (12).

3. (Currently amended) The method defined in Claim 2 wherein said link (19) is made without need for intermediate software layers.
4. (Currently amended) The method defined in Claim 3 includes in addition, the step of reading at least one of the following features embodied within said authentication system (16) : firmware programs, device-specific command sequences for execution of specific device-specific functions, cryptographic keys, cryptographic algorithms, and individual decision-making logic.
5. (Currently amended) The method defined in claim 4 which includes configuration of said devices; (12) by authorized persons, wherein after successful authentication, device-specific configuration data are downloaded into said devices (12) from said authentication system (16) in accordance with said authentication systems or over a network.
6. (Currently amended) A device (12) comprising the elements defined in Claim 5 for execution setting basic means of access for operations.
7. (Currently amended) An authentication system (16), created for authentication of a person or a group of people, comprising the elements defined in Claim 5.
8. (Currently amended) The authentication system (16) defined in Claim 7 which is implemented in the form of a SmartCard .
9. (Currently amended) A ~~System~~ system for setting basic means of access for operation of devices (12) of which the operation is controllable by electronic means, including at least one device (12) and an authentication system (16) as defined in Claim 8.

10. (Previously presented) A computer program, containing program code areas for the execution or preparation for execution of the steps of the method in accordance with Claim 4, when said program is installed in a computer.